Système d'accès à un réseau adapté pour la mise en œuvre d'un procédé à signature simplifiée, et serveur pour sa réalisation.

L'invention concerne un système d'accès à un réseau adapté pour la mise en œuvre d'un procédé à signature simplifiée, et un serveur pour sa réalisation.

Plus précisément, l'invention concerne un système comportant :

- au moins un poste d'utilisateur équipé d'un navigateur internet,
- un serveur proxy par lequel passent tous les flux d'informations échangés entre le ou chaque poste d'utilisateur et ledit réseau,
- plusieurs fournisseurs de services raccordés audit réseau, chaque fournisseur de services étant apte à émettre une requête d'authentification vers le poste de l'utilisateur qui le contacte pour identifier et/ou authentifier cet utilisateur avant de lui fournir des services personnalisés et/ou sécurisés, la réponse à fournir par un même utilisateur à cette requête d'authentification pouvant être différente en fonction du fournisseur de services contacté,
- au moins un serveur d'authentification propre à mémoriser au moins une information d'authentification pour chaque utilisateur et à transmettre en réponse à une requête d'authentification une réponse d'authentification contenant une information d'authentification fonction à la fois du fournisseur de services ayant émis la requête d'authentification, et de l'identité de l'utilisateur ayant contacté ce fournisseur de services, et
- un module à signature simplifiée apte à traiter automatiquement en lieu et place du ou de chaque poste d'utilisateur les requêtes d'authentification émises par les fournisseurs de services contactés, ce module étant apte pour chaque utilisateur :
  - à diriger les requêtes d'authentification vers le serveur d'authentification approprié, et
  - à retransmettre au fournisseur de services la réponse d'authentification correspondante transmise par le serveur d'authentification approprié.

Ces systèmes permettent de mettre en œuvre un procédé à signature simplifiée plus connu sous les termes de procédé SSO ("Single Sign On" ou "Simplified Sign On"). Des renseignements plus précis sur un exemple de procédé SSO peuvent être obtenus à la lecture des recommandations définies par le consortium d'entreprises appelé Liberty Alliance, dont le but est le développement des transactions sur Internet. Ces recommandations peuvent par exemple, être obtenues à partir du site Internet http://www.projectliberty.org.

Les procédés SSO visent à simplifier l'identification et/ou l'authentification d'un utilisateur sur la toile d'araignée mondiale plus connue sous les termes de WEB (World Wide Web). Dans la suite de cette description, la toile d'araignée mondiale sera simplement désignée par le terme réseau internet.

Les procédés SSO et notamment ceux conformes aux recommandations de Liberty Alliance, implémentent le module à signature simplifiée dans le serveur proxy. Toutefois, cette solution présente l'inconvénient qu'elle implique des modifications substantielles des serveurs proxy existants et qu'elle suppose une augmentation des traitements à réaliser par les serveurs proxy existants.

L'invention vise à remédier à cet inconvénient en proposant un système d'accès à un réseau à commutation de paquets adapté pour la mise en œuvre d'un procédé SSO dans lequel les modifications à apporter au serveur proxy sont mineures et les conséquences sur la charge à traiter sont mineures.

L'invention a donc pour objet un système tel que décrit ci-dessus, caractérisé en ce qu'il comporte un serveur supplémentaire indépendant du serveur proxy, le module à signature simplifiée étant implémenté dans ce serveur supplémentaire, et en ce que le serveur proxy est équipé d'une interface permettant de raccorder le serveur supplémentaire et de transmettre au moins les requêtes d'authentification émises par les fournisseurs de services contactés audit serveur supplémentaire pour traitement de ces requêtes par le module à signature simplifiée.

Suivant d'autres caractéristiques du système conforme à l'invention, celui-ci se caractérise en ce que :

- le module à signature simplifiée comporte un sous-module propre à identifier l'utilisateur à partir de son adresse réseau et à ajouter un identificateur de l'utilisateur aux requêtes d'authentification dirigées vers les serveurs d'authentification ;

- ladite au moins une information d'authentification mémorisée pour chaque utilisateur comprend une information sur un niveau d'authentification disponible pour cet utilisateur, en ce que chaque requête d'authentification émise par un fournisseur de services spécifie des caractéristiques sur le niveau d'authentification requis par ce fournisseur de services pour pouvoir accéder aux services qu'il propose, en ce que le ou chaque serveur d'authentification est apte à comparer les caractéristiques sur le niveau d'authentification requis spécifié par la requête d'authentification à l'information sur le niveau d'authentification disponible, de manière à déterminer si le niveau d'authentification requis correspond au niveau d'authentification disponible pour cet utilisateur, et en ce que le ou chaque serveur d'authentification est apte à émettre vers l'utilisateur une requête d'authentification active propre à activer sur le poste de l'utilisateur un processus interactif d'identification et/ou d'authentification de l'utilisateur si le niveau d'authentification requis ne correspond pas au niveau d'authentification disponible ;

- le serveur supplémentaire comporte un sous-module propre à diriger la réponse de l'utilisateur aux requêtes d'authentification active vers le serveur d'authentification qui l'a émise ;

- le serveur supplémentaire comporte un sous module propre à diriger la requête d'authentification active vers le poste de l'utilisateur ;

- le module à signature simplifiée comporte un sous-module capable d'ajouter aux requêtes transmises par le poste d'utilisateur vers un fournisseur de services un signal d'identification de service à signature simplifiée en réponse auquel le fournisseur de services émet la requête d'authentification ;

- le serveur supplémentaire et le serveur proxy sont aptes à communiquer l'un avec l'autre en mettant en œuvre un protocole de transfert de flux HTTP (Hyper Text Transfer Protocol) ;

- le protocole de transfert de flux HTTP est le protocole iCAP (Internet Content Adaptation Protocol) ou le protocole OCP (OPES Call Out Protocol).

- le serveur supplémentaire est uniquement apte à communiquer avec les fournisseurs de services par l'intermédiaire du protocole de transfert de flux HTTP mis en œuvre entre lui et le serveur proxy ;

- le serveur supplémentaire implémente également un serveur et/ou un client HTTP (Hyper Text Transfer Protocol) pour communiquer directement avec le ou chaque fournisseur de services et/ou le ou chaque serveur d'authentification uniquement à l'aide du protocole HTTP ;

- il comporte un fournisseur d'accès audit réseau auquel doit se connecter le ou chaque poste d'utilisateur pour pouvoir accéder audit réseau, ce fournisseur d'accès étant équipé du serveur proxy ;

- ledit réseau est la toile d'araignée mondiale.

L'invention sera mieux comprise à la lecture de la description qui va suivre donnée uniquement à titre d'exemple et faite en se référant aux dessins sur lesquels :

- la figure 1 est une illustration schématique de l'architecture d'un système conforme à l'invention,

- la figure 2 est un organigramme d'un procédé à signature simplifiée mis en œuvre dans le système de la figure 1, et

- les figures 3 et 4 sont des illustrations schématiques de la circulation des flux d'informations entre les différents équipements du système de la figure 1.

La figure 1 représente un système, désigné par la référence générale 2, d'accès à un réseau 4 à commutation de paquets adapté pour la mise en œuvre d'un procédé SSO conforme aux recommandations définies par Liberty Alliance.

Les recommandations établies par Liberty Alliance définissent l'organisation et les fonctionnalités des différents équipements ou groupes d'équipements du système 2 avec une précision suffisante pour que l'homme du métier à la lecture de ces recommandations puisse fabriquer ses équipements. Ces recommandations ne décrivent pas la réalisation détaillée de

chacun de ces équipements. Par conséquent, dans la suite de la description, on ne décrira de façon détaillée que le bloc d'équipement représenté par un rectangle en pointillé sur la figure 1, les autres équipements du système 2 étant réalisés de façon conventionnelle à partir des recommandations de Liberty Alliance.

Le système 2 sera ici décrit dans le cas particulier où le réseau 4 est le réseau internet.

Le système 2 comporte de nombreux postes d'utilisateurs ayant des fonctionnalités similaires les unes aux autres ainsi que plusieurs fournisseurs d'accès internet, ayant également des fonctionnalités similaires les unes aux autres. Ici pour simplifier l'illustration de la figure 1, seul un poste d'utilisateur 10 et un fournisseur d'accès 12 ont été représentés.

Le poste 10 est apte à naviguer sur le réseau 4. A cet effet, il est formé, par exemple, d'un ordinateur conventionnel 14 équipé d'un écran et d'un clavier ainsi que d'un navigateur internet 16 plus connu sous le terme anglais de "browser".

Le système 2 comporte également de nombreux systèmes fournisseurs de services ainsi que plusieurs serveurs d'authentification. Ici, seuls deux systèmes fournisseurs de services 20, 22, désignés fournisseurs, ainsi que deux serveurs d'authentification 24, 26 sont représentés sur la figure 1 pour simplifier l'illustration.

Les fournisseurs de services 20, 22 sont destinés à rendre des services à l'utilisateur du poste 10.

Par exemple, ici, le fournisseur 20 est un serveur informatique propre à établir des fiches de paye en fonction des informations qui lui sont communiquées par l'utilisateur du poste 10. Pour cela, le serveur 20 comporte un module 32 propre à identifier et à authentifier l'utilisateur du poste 10 de manière à personnaliser et à sécuriser le service qu'il rend à cet utilisateur. Plus précisément, le fournisseur 20 est associé à une mémoire 30 dans laquelle est enregistrée une liste 34 de serveurs d'authentification connus du fournisseur 20 ainsi qu'un niveau 36 d'authentification requis par ce fournisseur.

La liste 34 comporte des identificateurs des serveurs d'authentification contenant des informations d'authentification propres à

identifier et authentifier un utilisateur auprès de ce fournisseur de services. Une telle information est, par exemple, un niveau d'authentification disponible actuellement pour un utilisateur donné.

Le niveau d'authentification enregistré dans la mémoire 30 définit la qualité de l'authentification requise par le fournisseur 20. Dans le système 2, à titre d'exemple, chaque niveau d'authentification peut prendre l'une quelconque des valeurs entières comprises entre "1" et "5". Plus la valeur du niveau d'authentification est petite, plus la qualité de l'authentification est faible. Ici, à titre d'exemple, le niveau d'authentification 36 est égal à "2".

Les fonctions réalisées par le module 32 sont décrites plus en détail en regard des figures 3 et 4 et l'intérêt de la liste 34 ainsi que du niveau d'authentification apparaîtra à la lecture de la suite de cette description. On mentionnera ici simplement le fait que le module 32 est capable d'émettre une requête d'authentification HTTP incluse dans une réponse HTTP pour authentifier l'utilisateur vers le poste 10 de cet utilisateur.

Le fournisseur 22 permet, par exemple, à l'utilisateur du poste 10 de gérer à distance ses comptes bancaires et d'effectuer également des transactions bancaires. Le fournisseur 22 comporte les mêmes éléments que ceux décrits en regard du fournisseur 20 à l'exception du fait que le niveau d'authentification 36 est remplacé par un niveau d'authentification 38 égal à "4".

Les serveurs d'authentification 24 et 26 sont destinés à répondre aux requêtes d'authentification émises par les fournisseurs de services. A cet effet, les serveurs 24 et 26 sont associés chacun à une mémoire 40, 41 dans laquelle est enregistrée pour chaque utilisateur connu de ce serveur, une information 42, 43 d'authentification. Chaque information d'authentification contient le niveau d'authentification disponible pour l'utilisateur correspondant.

Chaque serveur d'authentification 24, 26 comporte également un module 44 de contrôle d'accès. Ce module permet aux serveurs 24 et 26 d'émettre une requête d'authentification active de manière à interroger l'utilisateur du poste 10 pour que celui-ci fournisse un jeu d'informations permettant de l'identifier et de l'authentifier avec un niveau d'authentification souhaité. Un jeu d'informations est, par exemple, un identificateur de l'utilisateur et son mot de passe.

Ces serveurs d'authentification sont connus sous les termes anglais "Identity provider".

Le fournisseur d'accès 12 est capable de remplir les fonctions classiques d'un fournisseur d'accès internet, c'est-à-dire notamment d'affecter une adresse réseau au poste 10 pour que celui-ci puisse naviguer sur le réseau 4.

A cet effet, il comporte un serveur proxy HTTP (Hyper Text Transfer Protocol) et un serveur 52 de contrôle d'accès. Le protocole HTTP existant est un protocole de communication utilisé pour les échanges de données entre des clients HTTP et des serveurs HTTP connus sous les termes de serveur web. Le serveur proxy est placé en coupure de flux entre le poste 10 et le réseau 4, c'est-à-dire que l'ensemble des flux d'informations échangés entre le navigateur 16 du poste 10 et le réseau 4 passe par l'intermédiaire du serveur proxy 50. Ainsi, le serveur proxy 50 voit passer l'ensemble des requêtes et des réponses HTTP émises par le poste 10 ou vers le poste 10.

Le serveur de contrôle d'accès 52 est capable d'identifier et d'authentifier l'utilisateur du poste 10 avant d'autoriser ce poste 10 à se connecter au réseau 4 et à naviguer sur celui-ci. Typiquement, l'utilisateur du poste 10 s'identifie auprès du serveur 52 en fournissant un jeu d'informations contenant un identificateur connu sous le terme anglais de "login" et un mot de passe. Si l'utilisateur est correctement identifié et authentifié, c'est-à-dire que le jeu informations qu'il a fourni correspond à un abonnement valide auprès de ce fournisseur d'accès, le serveur 52 affecte à cet utilisateur une adresse réseau, c'est-à-dire ici une adresse IP (Internet Protocol) pour naviguer sur le réseau 4. Dans le cas contraire, le serveur 52 interdit toute connexion au réseau 4.

Le serveur 52 est également capable d'enregistrer dans une mémoire 54 à laquelle il est associé une liste 56 contenant pour chaque adresse IP affectée à un utilisateur, l'identificateur de l'utilisateur correspondant. Cette liste est mise à jour automatiquement par le serveur 52.

Le fournisseur d'accès 12 comporte un serveur iCAP 60 (Internet Content Adaptation Protocol) placé à côté du serveur 50 et raccordé à celui-ci par l'intermédiaire d'une liaison filaire 62 ou d'un réseau local. Le protocole iCAP existant est normalisé par l'organisme IETF (Internet Engineering Task

Force) pour la transformation systématique de contenus sur Internet. Ainsi, le serveur 60 et le serveur 50 sont capables de communiquer l'un avec l'autre en mettant en œuvre le protocole iCAP. Plus précisément, le serveur 50 est apte à communiquer au serveur 60 des requêtes ou des réponses HTTP présentes dans les flux d'informations échangés entre le poste 10 et le réseau 4 et le serveur 60 est également capable de transmettre des requêtes ou des réponses HTTP après les avoir modifiées au serveur 50.

De manière à implémenter un client iCAP dans le serveur proxy 50 celui-ci est équipé d'une interface iCAP 64 comportant un connecteur permettant de le raccorder au serveur 60.

L'interface 64 est ici configurée pour transmettre au serveur 60 uniquement les requêtes ou les réponses HTTP qui doivent être modifiées pour la mise en œuvre du procédé SSO.

Le serveur 60 est équipé d'un module SSO 66 propre à prendre en charge tous les traitements spécifiques requis par la mise en œuvre du procédé SSO. Ce module 66 comporte trois sous-modules 68, 70 et 72 correspondant chacun à un service iCAP. Ces sous-modules seront décrits plus en détail en regard de chacune des figures 3 et 4.

Le serveur 60 est associé à la mémoire 54 qui contient également une liste 76 des serveurs d'authentification connus par chaque utilisateur. Cette liste 76 regroupe pour chaque utilisateur, les identificateurs des différents serveurs d'authentification dans lesquels sont mémorisées des informations d'authentification pour cet utilisateur.

Le serveur 60 implémente aussi un client HTTP. A cet effet, il est raccordé au réseau 4 par l'intermédiaire d'un serveur proxy HTTP supplémentaire 74 qui peut être indépendant et distinct du serveur proxy 50.

L'ensemble des serveurs du système 2 sont réalisés à partir de calculateurs électroniques conventionnels programmables aptes à exécuter des instructions enregistrées sur un support d'enregistrement d'informations. A cet effet, les mémoires 30, 40, 41 et 54 comportent des instructions pour l'exécution du procédé SSO des figures 2 à 4 lorsque lesdites instructions sont exécutées par ces calculateurs.

Le fonctionnement du système 2 va maintenant être décrit en regard des figures 2 à 4.

Initialement, lors d'une étape 90, un identificateur du serveur 24 est enregistré dans la liste 76 des serveurs d'authentification connus par l'utilisateur.

Parallèlement, lors d'une étape 92, les listes 34 des fournisseurs de services sont mises à jour.

Ensuite, l'utilisateur du poste 10 se connecte, lors d'une étape 94, au réseau 4. Lors de cette étape, l'utilisateur saisit, lors d'une opération 96, un jeu d'informations permettant de l'identifier et de l'authentifier auprès du serveur 52.

Une fois que l'utilisateur 10 a été identifié et authentifié, le serveur 52, lors d'une opération 98, lui affecte une adresse IP et enregistre la relation entre cette adresse réseau et l'identificateur de cet utilisateur dans la liste 56.

Ensuite, le serveur 52 informe, lors d'une opération 100, les différents serveurs d'authentification connus par cet utilisateur que celui-ci a été correctement identifié et authentifié. Cette identification et authentification réalisée par le serveur 52 est ici associée à un niveau d'authentification égal à "2" de sorte que les serveurs d'authentification mémorisent que le niveau d'authentification disponible est égal à "2".

Une fois autorisé à naviguer sur le réseau 4, l'utilisateur se connecte, par exemple, lors d'une étape 104, au fournisseur de services 20. Le module 32 du fournisseur 20 émet alors en réponse, lors d'une opération 106, une requête d'authentification HTTP incluse dans une réponse HTTP à destination du poste 10. Cette requête est interceptée par le serveur proxy 50 puis traitée par le serveur iCAP 60 et enfin transmise jusqu'au serveur d'authentification 24. Cette requête d'authentification comporte le niveau d'authentification 36. Le serveur 24 vérifie, lors d'une étape 108, que le niveau d'authentification disponible pour cet utilisateur est au moins égal à "2". Ici, le niveau d'authentification disponible étant égal à celui requis par le fournisseur 20, le serveur 24 transmet, lors d'une étape 110, une réponse d'authentification contenant un certificat d'authentification au fournisseur 20. Ce certificat informe le fournisseur 20 que le niveau d'authentification requis est disponible.

Le fournisseur 20 ayant reçu le certificat propose alors, lors d'une étape 112, à cet utilisateur un service personnalisé et / ou sécurisé sans que l'utilisateur ait besoin de s'identifier auprès du fournisseur 20. Par exemple, le fournisseur 20 lui propose l'impression d'une feuille de paye comportant son nom.

Ensuite, toujours lors de la même connexion, l'utilisateur 10 se connecte en 114 au fournisseur de services 22. Ce fournisseur 22 exécute alors l'opération 106.

Toutefois, contrairement au cas précédent, le serveur d'authentification 24 constate que le niveau d'authentification requis par le fournisseur 22 est supérieur à celui actuellement disponible pour cet utilisateur.

Le module 44 de contrôle d'accès du serveur 24 procède alors à une étape 120 d'authentification active lors de laquelle il interroge l'utilisateur, de manière à identifier et à authentifier celui-ci avec une qualité d'authentification correspondant au niveau d'authentification "4". Par exemple, le module 44 demande à l'utilisateur de saisir des informations personnelles telles que sa date de naissance.

Si l'utilisateur du poste 10 a été correctement identifié et authentifié avec un niveau d'authentification "4", le serveur 24 enregistre le nouveau niveau d'authentification disponible dans sa mémoire 40 et procède à l'étape 110.

Ensuite, le fournisseur 22 propose lors d'une étape 122 un service personnalisé et / ou sécurisé à cet utilisateur.

Le procédé ci-dessus décrit dans le cas particulier des fournisseurs 20, 22, est alors réitéré au fur et à mesure que l'utilisateur du poste 10 contacte de nouveaux fournisseurs de services.

Ainsi, grâce à ce procédé, l'authentification de l'utilisateur est simplifiée puisque celui-ci ne doit s'identifier et s'authentifier que lors de la connexion au réseau 4 puis ensuite à chaque fois qu'il contacte un fournisseur de services exigeant un niveau d'authentification supérieur à celui disponible. Ce procédé permet donc d'éviter à l'utilisateur de saisir, à chaque fois qu'il contacte un nouveau fournisseur de services, un jeu d'informations d'identification et d'authentification correspondant à ce fournisseur de services.

Les flux d'informations échangés entre les équipements du système 2 lors des étapes 104 à 122 vont maintenant être décrits plus en détails en regard des figures 3 et 4.

Sur les figures 3 et 4 les blocs rectangulaires représentent des équipements ou des listes mémorisées déjà décrites en regard de la figure 1 et portent donc les mêmes références. Les flèches entre ces équipements représentent à la fois le sens de circulation des informations et les opérations correspondantes.

Initialement, le navigateur 16 du poste 10 envoie une requête HTTP vers le module 32 d'un fournisseur de services, par exemple le fournisseur 20. Cette requête est acheminée, lors d'une opération 130, jusqu'au serveur proxy 50. L'interface 64 intercepte cette requête et la transmet, lors d'une opération 132, au serveur 60 et plus précisément au sous-module 68. Le sous-module 68 ajoute un en-tête à la requête HTTP indiquant que le système 2 supporte un procédé SSO et retransmet, lors d'une opération 134 cette requête HTTP ainsi modifiée vers le serveur proxy 50.

Le serveur proxy transmet alors la requête HTTP modifiée jusqu'au fournisseur de services lors d'une opération 136.

Le module 32 du fournisseur de services détecte la présence de l'en-tête ajouté par le sous-module 68 et, en réponse, envoie, lors d'une opération 138, une requête d'authentification vers le navigateur 16.

La requête d'authentification est, par exemple, conforme au protocole SOAP (Single Object Access Protocol) normalisé par l'organisme W3C (World Wide Web Consortium).

Cette requête d'authentification comporte notamment un identifiant du fournisseur de services, une copie de la liste 34 de serveurs d'authentification connus, le niveau d'authentification requis par ce fournisseur et, par exemple, une instruction connue sous les termes anglais "set cookie" destinée à enregistrer un identificateur de la requête d'authentification sur le poste 10 ou, en variante, directement un identifiant de la requête.

L'interface 64 du serveur proxy 50 intercepte cette requête d'authentification et la dirige, lors d'une opération 140, vers le sous-module 70 du serveur 60.

Le sous-module 70 compare, lors d'une opération 142, la liste 34 reçue à la liste 56 pour sélectionner le serveur d'authentification à contacter, par exemple, ici le serveur 24. S'il n'existe aucun serveur d'authentification commun à la liste 34 reçue et à la liste 56, le sous-module 70 envoie un message d'incompatibilité au fournisseur de services ayant émis la requête d'authentification. Ce message d'incompatibilité comporte l'identificateur de la requête d'authentification, de manière à ce que le module 32 puisse relier cette réponse à la requête d'authentification correspondante. L'identificateur de la requête d'authentification est, par exemple, celui contenu dans l'instruction "set cookie".

Ensuite, le sous-module 70 détermine, lors d'une opération 144, l'identité de l'utilisateur du poste 10 en comparant l'adresse réseau du poste 10 à la liste 76. Cette adresse aura été fournie par le serveur proxy 50 au sous-module 70 lors de l'opération 140 par l'intermédiaire d'un champ de l'en-tête HTTP.

Une fois l'utilisateur identifié, le sous-module 70 procède à une opération 148 de transmission de la requête d'authentification reçue associée à l'identificateur de l'utilisateur obtenu lors de l'opération 144, au serveur d'authentification sélectionné lors de l'opération 142.

Le serveur 24 compare, lors d'une opération 150, le niveau d'authentification disponible pour l'utilisateur à celui requis par le fournisseur de services.

Dans le cas où le niveau d'authentification requis est supérieur à celui actuellement enregistré par le serveur 24, celui-ci procède comme décrit en regard de la figure 4.

Dans le cas contraire, le serveur 24 envoie lors d'une opération 152, une réponse d'authentification au serveur 60.

Le sous-module 70 reçoit la réponse d'authentification et la transmet, lors d'une opération 156, vers le fournisseur de services par l'intermédiaire du serveur proxy 74 et en utilisant le protocole HTTP. Cette réponse d'authentification comporte si nécessaire un identificateur de l'utilisateur.

Le fournisseur de services répond à cette réponse d'authentification en transmettant vers le serveur 60, lors d'une opération 158, par exemple, une

page d'accueil personnalisée. Cette réponse est transmise par l'intermédiaire du serveur proxy 74 au serveur 60 en utilisant le protocole HTTP.

Le sous-module 70 redirige, lors d'une opération 160, cette réponse vers le serveur proxy 50 en utilisant le protocole iCAP qui la redirige, à son tour, lors d'une opération 162, vers le navigateur 16 en utilisant le protocole HTTP.

Ainsi, une page d'accueil personnalisée s'affiche sur le navigateur 16 de l'utilisateur du poste 10 sans même que cet utilisateur ait eu besoin de s'identifier auprès, par exemple, du fournisseur 20.

La figure 4 représente la circulation des informations entre les différents équipements du système 2 dans le cas particulier où le niveau d'authentification requis par le fournisseur de services contacté est supérieur à celui actuellement mémorisé dans la mémoire 40 du serveur 24. Sur cette figure, les équipements et les opérations déjà décrits en regard des figures 1 et 3 portent les mêmes références et les nouvelles opérations sont représentées en traits gras.

Lors de l'opération 150, le serveur 24 a établi que le niveau d'authentification requis est supérieur à celui actuellement disponible pour l'utilisateur. Par conséquent, il procède à une opération 180 lors de laquelle le module 44 transmet une requête d'authentification active vers le serveur 60 contenue dans une réponse HTTP et en utilisant le protocole HTTP. La requête d'authentification active est destinée à activer sur le navigateur 16 un processus d'authentification interactif. A cet effet, cette requête comporte ici un formulaire à compléter par l'utilisateur.

Le sous-module 70 retransmet lors d'une opération 182, cette requête d'authentification active vers le serveur proxy 50 en utilisant le protocole iCAP, puis le serveur proxy 50 la retransmet, lors d'une opération 184, vers le navigateur 16 en utilisant le protocole HTTP. Le navigateur 16 affiche le formulaire qui permet à l'utilisateur de s'identifier et de s'authentifier avec un niveau d'authentification supérieur, par exemple, égal à "4" dans le cas du fournisseur de services 22. Une fois que le formulaire a été complété, le navigateur 16 envoie, lors d'une opération 186, la réponse dans une requête HTTP. Cette réponse est interceptée par l'interface 64 du serveur 50 et transmise, lors d'une opération 188, au sous-module 72 en utilisant le protocole

iCAP. Le sous-module 72 retransmet alors, lors d'une opération 190, la réponse de l'utilisateur en utilisant le protocole HTTP au serveur 24. Si le formulaire a correctement été complété par l'utilisateur, c'est-à-dire que le jeu d'informations d'identification et d'authentification est correcte, le serveur 24 mémorise, lors d'une opération 192, le nouveau niveau d'authentification disponible dans la mémoire 40 et procède ensuite à l'opération 152. Les opérations suivantes sont identiques à celles décrites en regard de la figure 2 à l'exception du fait que les opérations 152, 156, 158 et 160 font intervenir le sous-module 72 à la place du sous-module 70.

La plupart des serveurs proxy existant comportent déjà une interface iCAP. Ainsi, le système de la figure 2 simplifie la mise en œuvre du procédé SSO puisque la seule modification à apporter au serveur proxy consiste à le configurer de manière à ce que l'interface iCAP intercepte les requêtes HTTP nécessaires à la mise en œuvre de ce procédé.

La circulation des flux d'informations entre les différents éléments du système 2 a été décrite dans le cas particulier où le serveur iCAP 60 communique directement en utilisant le protocole HTTP avec le ou les fournisseurs de services lors des opérations 156 et 158. En variante, le serveur iCAP communique avec les fournisseurs de services uniquement par l'intermédiaire du protocole iCAP. Par exemple, dans cette variante, les requêtes HTTP émises à destination du fournisseur de services lors de l'opération 156 sont d'abord transmises par le serveur 60 jusqu'au serveur proxy 50 en utilisant le protocole iCAP puis le serveur proxy 50 transmet ces requêtes au fournisseur de services en utilisant le protocole HTTP. La réponse HTTP émise par le fournisseur de services lors de l'opération 158 suit le chemin inverse de la requête émise lors de l'opération 156. Dans cette variante, le serveur 60 ne communique jamais directement avec les fournisseurs de services de sorte que ceux-ci ne sont pas au courant de l'existence du serveur 60. L'utilisation du serveur 60 est alors totalement transparente pour ces fournisseurs de services. Cette variante présente l'avantage que du point de vue du fournisseur de services, tous les échanges d'informations se font entre lui et l'utilisateur sans avoir connaissance de l'existence du serveur 60. Cette variante présente également l'avantage que les requêtes HTTP émises et

reçues lors des opérations 156 et 158 sont directement échangées avec le serveur proxy 50 et non plus par l'intermédiaire du sous-module 70 ce qui accélère le traitement de ces opérations.

Les sous-modules 68 à 72 ont été décrits dans le cas particulier où ils sont tous implémentés dans le même serveur iCAP 60. En variante, ces sous-modules sont chacun implémentés dans un serveur iCAP indépendant des autres.

Ici, l'interface 64 est configurée pour n'intercepter que les requêtes HTTP qui doivent être traitées par le serveur iCAP. En variante, l'interface 64 est configurée pour rediriger tous les flux d'informations HTTP vers le serveur iCAP et le serveur iCAP implémente un module de filtrage propre à envoyer au module de traitement 66 uniquement les requêtes HTTP qui doivent être traitées par ce module. Ainsi, dans cette variante, l'interception des requêtes HTTP n'est pas réalisée par le serveur proxy 50 mais par le serveur iCAP.

Le système 2 a été représenté dans le cas particulier où les serveurs d'authentification sont raccordés au fournisseur d'accès internet par l'intermédiaire du réseau 4. En variante, au moins l'un de ces serveurs d'authentification est logé chez le fournisseur d'accès internet et raccordé à celui-ci par l'intermédiaire d'un réseau local indépendant du réseau 4. Ce mode de mise en œuvre avantageux lui permettra de bénéficier de toutes les identifications / authentifications réalisées par le fournisseur d'accès et qui ne pourraient être partagées avec des fournisseurs d'authentification externes pour des raisons de sécurité;

De même, en variante, le serveur iCAP est raccordé au serveur proxy 50 par l'intermédiaire d'un réseau grande distance et non plus par l'intermédiaire d'une liaison ou d'un réseau local.

Le système 2 a été décrit dans le cas particulier où la première authentification de chaque utilisateur est réalisée par le fournisseur d'accès internet 12. En variante, cette première authentification n'est plus réalisée par le fournisseur d'accès internet 12 mais, par exemple, par le premier fournisseur de services contacté par l'utilisateur.

L'identification et l'authentification de l'utilisateur ont été décrites dans le cas particulier où celle-ci se fait à partir d'un terminal 10 équipé d'un

écran et d'un clavier ce qui permet de saisir un jeu d'informations d'identification et d'authentification. En variante, la première identification et authentification de l'utilisateur est réalisée automatiquement, par exemple, en identifiant le terminal utilisé par cet utilisateur. Plus précisément, lorsque le terminal 10 est remplacé par un téléphone mobile, l'identification et l'authentification de l'utilisateur se font automatiquement en procédant à l'acquisition du numéro de téléphone du terminal. Dans ce cas, l'authentification est dite transparente.

Le système 2 a également été décrit dans le cas particulier où les serveurs d'authentification mémorisent uniquement le niveau d'authentification disponible pour chaque utilisateur ce qui renforce la sécurité du système puisqu'il n'est pas désirable que l'ensemble des mots de passe et autres informations secrètes de l'utilisateur soient enregistrés dans un même lieu. Toutefois, en variante, ces serveurs d'authentification mémorisent également en tant qu'informations d'authentification le ou les jeux d'informations d'identification et d'authentification que chaque utilisateur est susceptible d'utiliser pour s'identifier et s'authentifier auprès de chaque fournisseur de services. Ainsi, dans cette variante, la réponse d'authentification comporte le jeu d'informations d'identification et d'authentification à transmettre au fournisseur de services pour que celui-ci identifie et authentifie l'utilisateur. Ce jeu d'informations d'identification et d'authentification est transmis au fournisseur de services de façon similaire a ce qui a été décrit pour le certificat d'authentification.

Le système 2 a été décrit dans le cas particulier où la requête d'authentification émise par chaque fournisseur de services comporte un niveau d'authentification. En variante, la requête d'authentification émise par l'un des fournisseurs de services ne comporte pas de niveau d'authentification. Dans cette variante, en réponse à cette requête d'authentification, le serveur d'authentification contacté fournit, en réponse, un certificat d'authentification indiquant simplement que l'utilisateur a été authentifié. Ainsi, dans cette variante, l'utilisateur aura accès aux services du fournisseur de services à partir du moment où il a été authentifié au moins une fois et ceci quel que soit le niveau de cette authentification.

Le système 2 a été décrit dans le cas particulier où le réseau 4 est le réseau internet. Toutefois en variante, ce réseau 4 est un réseau de transmission d'informations quelconque tel qu'un réseau local, un réseau à commutation de paquets quelconque ou un réseau à commutation de circuits.

Le système 2 a été décrit dans le cas particulier où les serveurs d'authentification sont aptes à émettre des requêtes d'authentification actives lorsque ceux-ci ne disposent pas d'une authentification satisfaisante pour l'utilisateur. En variante, les serveurs d'authentification ne sont pas aptes à émettre ces requêtes d'authentification actives. Dès lors, dans cette variante, lorsqu'un serveur d'authentification est contacté alors qu'il ne possède, par exemple, aucune information d'authentification sur l'utilisateur, il est apte à émettre un message d'erreur à la place d'une requête d'authentification active.

Finalement, le système 2 a été décrit dans le cas particulier où le protocole de transfert de flux HTTP est le protocole iCAP. En variante, le protocole iCAP peut être remplacé par tout autre protocole de transfert de flux HTTP tel que par exemple le protocole OCP (OPES Call Out Protocol) avec OPES (Open Pluggable Edge Services).

Le système 2 a été défini en faisant référence aux recommandations établies par Liberty Alliance. Toutefois, l'invention revendiquée n'est pas limitée aux systèmes et aux procédés conformes aux recommandations de Liberty Alliance et s'applique à tout système ou procédé présentant des fonctionnalités similaires à celles décrites ici.

REVENDICATIONS

1. Système d'accès à un réseau (4) à commutation de paquets adapté pour la mise en œuvre d'un procédé à signature simplifiée, ce système comportant :

- un serveur proxy (50) par lequel passent tous les flux d'informations échangés entre un utilisateur et ledit réseau,
- plusieurs fournisseurs (20, 22) de services raccordés audit réseau (4), chaque fournisseur de services étant apte à émettre une requête d'authentification vers l'utilisateur qui le contacte pour identifier et/ou authentifier cet utilisateur avant de lui fournir des services personnalisés et/ou sécurisés, la réponse à fournir par un même utilisateur à cette requête d'authentification pouvant être différente en fonction du fournisseur de services contacté,
- au moins un serveur d'authentification (24, 26) propre à mémoriser au moins une information d'authentification pour chaque utilisateur et à transmettre en réponse à une requête d'authentification une réponse d'authentification contenant une information d'authentification fonction à la fois du fournisseur de services ayant émis la requête d'authentification, et de l'identité de l'utilisateur ayant contacté ce fournisseur de services, et
- un module (66) à signature simplifiée apte à traiter automatiquement en lieu et place de l'utilisateur les requêtes d'authentification émises par les fournisseurs de services contactés, ce module étant apte pour chaque utilisateur :
  - à diriger les requêtes d'authentification vers le serveur d'authentification (24, 26) approprié, et
  - à retransmettre au fournisseur de services la réponse d'authentification correspondante transmise par le serveur d'authentification approprié,

caractérisé en ce qu'il comporte un serveur supplémentaire (60) indépendant du serveur proxy (50), le module à signature simplifiée (66) étant implémenté dans ce serveur supplémentaire (60), et en ce que le serveur proxy (50) est équipé d'une interface (64) permettant de le raccorder au serveur

supplémentaire (60) et de transmettre au moins les requêtes d'authentification émises par les fournisseurs de services contactés audit serveur supplémentaire (60) pour traitement de ces requêtes par le module à signature simplifiée (66).

2. Système selon la revendication 1, caractérisé en ce que le module à signature simplifiée (66) comporte un sous-module (70) propre à identifier l'utilisateur à partir de son adresse réseau et à ajouter un identificateur de l'utilisateur aux requêtes d'authentification dirigées vers les serveurs d'authentification.

3. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite au moins une information d'authentification mémorisée pour chaque utilisateur comprend une information sur un niveau d'authentification disponible pour cet utilisateur, en ce que chaque requête d'authentification émise par un fournisseur de services (20, 22) spécifie des caractéristiques sur le niveau d'authentification requis par ce fournisseur de services pour pouvoir accéder aux services qu'il propose, en ce que le ou chaque serveur d'authentification (24, 26) est apte à comparer les caractéristiques sur le niveau d'authentification requis spécifié par la requête d'authentification à l'information sur le niveau d'authentification disponible, de manière à déterminer si le niveau d'authentification requis correspond au niveau d'authentification disponible pour cet utilisateur, et en ce que le ou chaque serveur d'authentification (24, 26) est apte à émettre vers l'utilisateur une requête d'authentification active propre à activer un processus interactif d'identification et/ou d'authentification de l'utilisateur si le niveau d'authentification requis ne correspond pas au niveau d'authentification disponible.

4. Système selon la revendication 3, caractérisé en ce que le serveur supplémentaire (60) comporte un sous-module (72) propre à diriger la réponse de l'utilisateur aux requêtes d'authentification active vers le serveur d'authentification qui l'a émise.

5. Système selon la revendication 3 ou 4 caractérisé en ce que le serveur supplémentaire comporte un sous module (70) propre à diriger la requête d'authentification active vers l'utilisateur.

6. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le module à signature simplifiée (66) comporte un sous-module (68) capable d'ajouter aux requêtes transmises par l'utilisateur vers un fournisseur de services un signal d'identification de service à signature simplifiée en réponse auquel le fournisseur de services émet la requête d'authentification.

7. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le serveur supplémentaire (60) et le serveur proxy (50) sont aptes à communiquer l'un avec l 'autre en mettant en œuvre un protocole de transfert de flux HTTP (Hyper Text Transfer Protocol).

8. Système selon la revendication 7, caractérisé en ce que le protocole de transfert de flux HTTP est le protocole iCAP (Internet Content Adaptation Protocol) ou le protocole OCP (OPES Call Out Protocol).

9. Système selon la revendication 7 ou 8, caractérisé en ce que le serveur supplémentaire (60) est uniquement apte à communiquer avec les fournisseurs de services par l'intermédiaire du protocole de transfert de flux HTTP mis en œuvre entre lui et le serveur proxy (50).

10. Système selon l'une quelconque des revendications 1 à 8, caractérisé en ce que le serveur supplémentaire (60) implémente également un serveur et/ou un client HTTP (Hyper Text Transfer Protocol) pour communiquer directement avec le ou chaque fournisseur de services et/ou le ou chaque serveur d'authentification uniquement à l'aide du protocole HTTP.

11. Système selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte un fournisseur d'accès (12) audit réseau (4) auquel doit se connecter l'utilisateur pour pouvoir accéder audit réseau, ce fournisseur d'accès étant équipé du serveur proxy (50).

12. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit réseau est la toile d'araignée mondiale.

13. Serveur supplémentaire apte à être mis en œuvre dans un système conforme à l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte le module à signature simplifiée (66) apte à traiter automatiquement en lieu et place de l'utilisateur les requêtes d'authentification émises par le ou chaque fournisseur de services contacté, et

est apte à communiquer avec un serveur proxy (50) pour recevoir au moins les requêtes d'authentification émises par les fournisseurs de services.

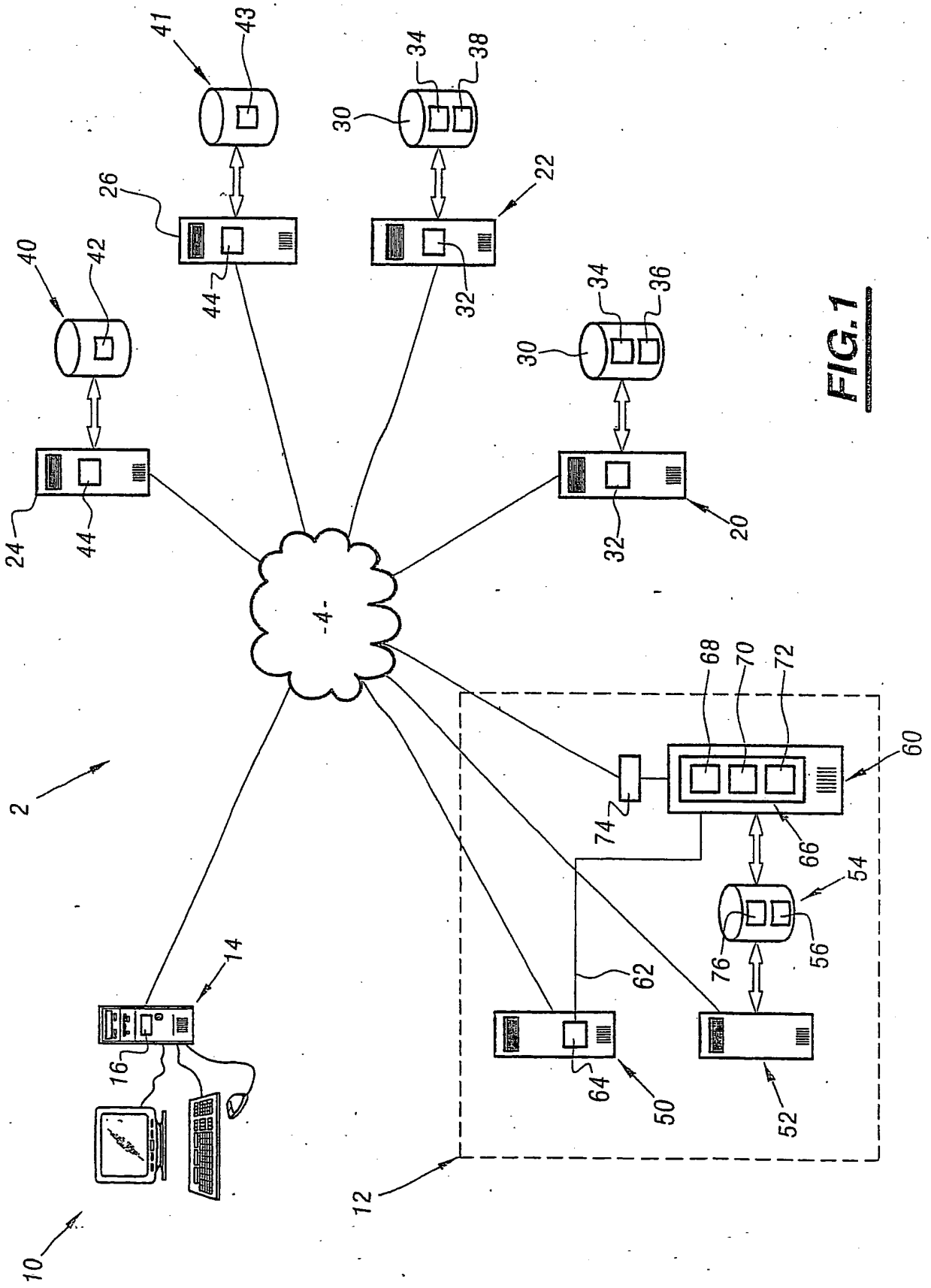
41
43
34
38
30
26
22
40
42
44
32
34
36
30
24
44
32
20
-4-
68
70
72
60
74
66
54
56
76
62
14
16
64
50
52
12
2
10

FIG.1

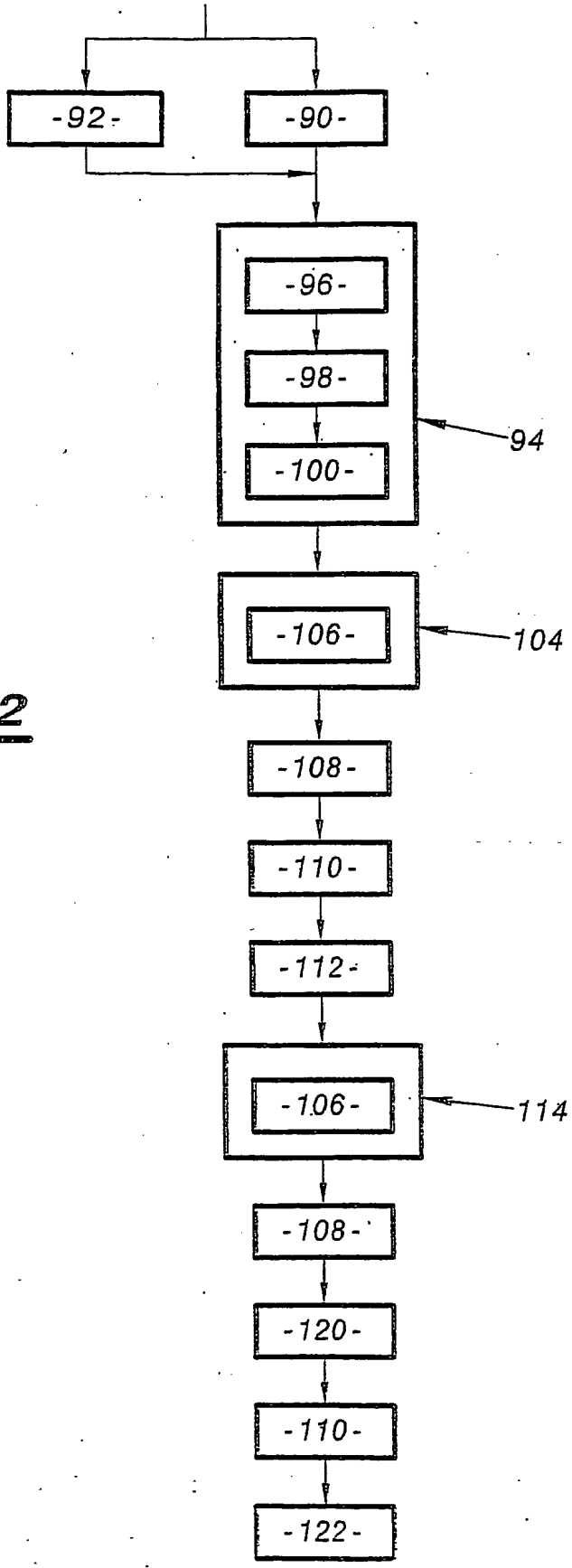

FIG.2

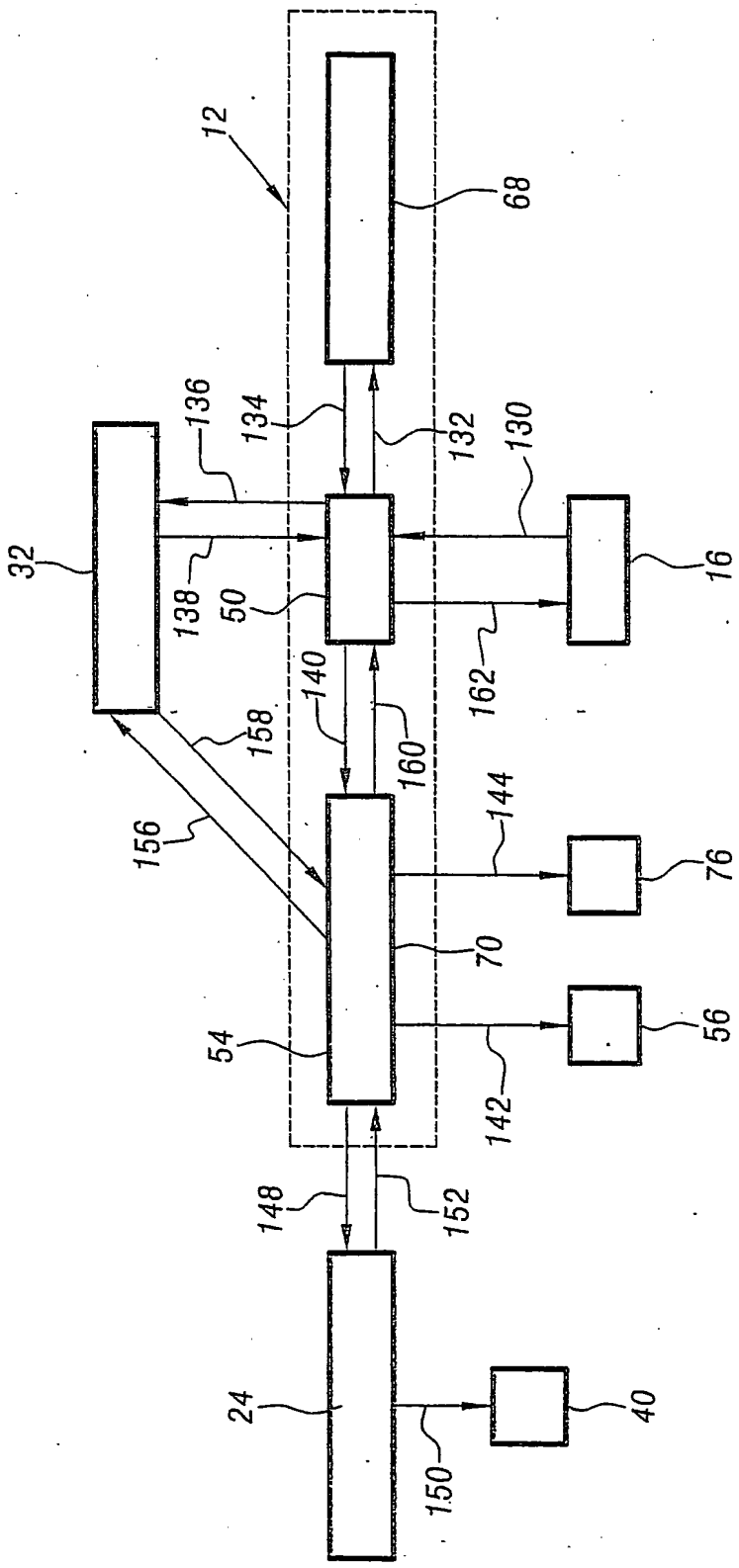
12
68
136
134
132
130
32
138
50
16
162
140
158
160
156
144
76
70
54
56
142
148
152
24
40
150

FIG.3

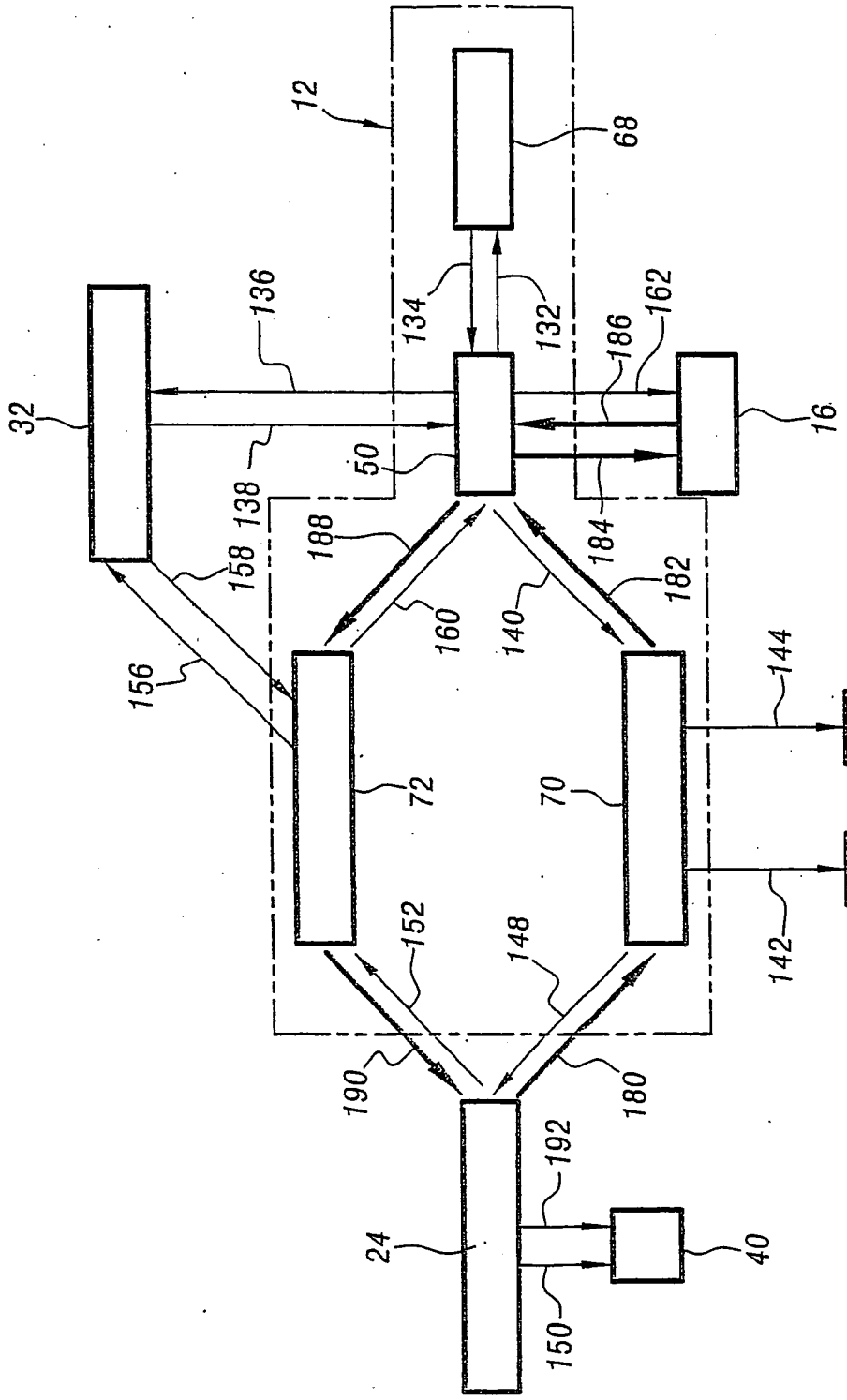
12
68
136
134
132
186
162
32
16
50
138
188
184
158
182
160
140
156
144
76
72
70
56
152
148
142
190
180
192
24
40
150

FIG.4

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/FR2004/002272

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/80067 A (YODLEE COM INC) 25 October 2001 (2001-10-25)	1,2,4-13
A	abstract figures 1,10 page 9, line 20 - page 10, line 6 page 17, line 16 - line 24 page 20, line 6 - line 25 page 22, line 8 - line 18 page 41, line 15 - page 45, line 24 claims 9-12,14	3
X	US 6 317 838 B1 (BAIZE ERIC) 13 November 2001 (2001-11-13)	1,2,4-13
A	abstract figure 2 column 3, line 50 - column 4, line 8 column 4, line 36 - line 54 column 5, line 13 - column 7, line 14	3
	-/—	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 January 2005	04/02/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Garcia Mahedero, P

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/002272

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/007460 A1 (AZUMA TOMIHIKO) 17 January 2002 (2002-01-17) abstract paragraph '0013! - paragraph '0015! paragraph '0087! - paragraph '0111!	1-13
A	"Liberty Architecture Overview, Version 1.1" LIBERTY PROJECT, 15 January 2003 (2003-01-15), XP002246163 Retrieved from the Internet: URL:http://projectliberty.org/specs/archive/v1_1/liberty-architecture-overview-v1.1> 'retrieved on 2003-07-02! the whole document	1-13

INTERNATIONAL SEARCH REPORT

mation on patent family members

Interna[redacted]al Application No
PCT/FR2004/002272

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0180067 A	25-10-2001	AU 4574401 A	30-10-2001
		WO 0180067 A1	25-10-2001
		US 2003187925 A1	02-10-2003
US 6317838 B1	13-11-2001	NONE	
US 2002007460 A1	17-01-2002	JP 2002032340 A	31-01-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/002272

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 2002/007460 A1 (AZUMA TOMIHIKO) 17 janvier 2002 (2002-01-17) abrégé alinéa '0013! - alinéa '0015! alinéa '0087! - alinéa '0111!	1-13
A	"Liberty Architecture Overview, Version 1.1" LIBERTY PROJECT, 15 janvier 2003 (2003-01-15), XP002246163 Extrait de l'Internet: URL:http://projectliberty.org/specs/archive/v1_1/liberty-architecture-overview-v1.1> 'extrait le 2003-07-02! le document en entier	1-13

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR2004/002272

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0180067	A	25-10-2001	AU	4574401 A	30-10-2001
			WO	0180067 A1	25-10-2001
			US	2003187925 A1	02-10-2003
US 6317838	B1	13-11-2001	AUCUN		
US 2002007460	A1	17-01-2002	JP	2002032340 A	31-01-2002